

STANDARDS AND PROCEDURES			ARIZONA DEPARTMENT OF ADMINISTRATION	IT DIVISIONS (ISD & ITSD)
Section:	06	Title:	Information Security	
Sub Section:	03	Title:	Information Security	
Document:	09	Title:	Software System Design or Purchase	

1. STANDARD

Appropriate information security and audit controls will be incorporated into all new software systems. Each phase of systems acquisition or in-house design will incorporate corresponding development or assurances of security and audibility controls.

1.1. Summary of Standard Changes

1.2. Purpose

Insure that all software used by ISD conforms to required security controls.

1.3. Scope

Applies to all software in use at ISD.

1.4. Responsibilities

1.5. Definitions and Abbreviations

1.6. Description of Standard

All software specifications will be authorized by the software owners. Proper security and audit controls will be included. Documentation will be prepared and authorized prior to development or purchase. Existing software undergoing re-development will have proper change control procedures in place.

1.7. Implications

Software or information owners will authorize all software and security specifications, and pre-documentation, prior to development or purchase. ISD will act as consultants in the specification process and will have approval rights in the area of security controls.

1.8. References

1.9. Attachments

2. BASIC SOFTWARE DESIGN PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. All software developed by in-house staff, or purchased for their use, which is intended to process sensitive information will have written formal specifications as

STANDARDS AND PROCEDURES			ARIZONA DEPARTMENT OF ADMINISTRATION	IT DIVISIONS (ISD & ITSD)
Section:	06	Title:	Information Security	
Sub Section:	03	Title:	Information Security	
Document:	09	Title:	Software System Design or Purchase	

part of an agreement between the involved information owner(s) and the system developer(s) or purchaser(s) prior to the beginning of development or purchase. The specifications will define:

2.2.1.1. Software functionality for users, developers, and auditors

2.2.1.2. Security control measures to be incorporated into the software

2.2.2. Users who develop or implement software will document the software in advance of its deployment. It will be written so that it may be run by persons unacquainted with it.

2.2.3. Necessary audit controls which will ensure proper software and information controls will be defined by owners and developers prior to the beginning of the project.

2.3. References

2.4. Attachments

3. SOFTWARE SECURITY AND AUDIT CONTROL DESIGN PROCEDURES

3.1. Summary of Procedure Changes

3.2. Procedure Details

3.2.1. The following security and audit controls will be addressed in writing, through a risk analysis, as part of the basic formal specifications prepared and signed prior to the project:

3.2.1.1. Determine sensitivity and criticality of the system information for the following;

3.2.1.1.1. security objectives

3.2.1.1.2. Assessing the threats, vulnerabilities, and risks to the system

3.2.1.2. Identify security requirements and select appropriate controls;

3.2.1.3. Develop security test plans;

3.2.1.4. Include approved security requirements and specifications in the development baselines;

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	03	Title: Information Security
Document:	09	Title: Software System Design or Purchase

- 3.2.1.5. Prepare documentation of security controls;
- 3.2.1.6. Ensure the removal of all 'back-doors' at the proper time during development phases;
- 3.2.1.7. Conduct acceptance tests and evaluations of system security during all development phases.

3.3. References

3.4. Attachments

4. SOFTWARE CHANGE PROCEDURES

4.1. Summary of Procedure Changes

4.2. Procedure Details

- 4.2.1. All changes to existing software will employ formal change control procedures that will ensure that only authorized changes are made and will include;
 - 4.2.1.1. Written authorization of written specifications by the information owner,
 - 4.2.1.2. Approved time frames of all aspects of the change process,
 - 4.2.1.3. The approved manner in which the changes will be made,
 - 4.2.1.4. The documentation of new processes (functional, security), and,
 - 4.2.1.5. Problem resolution and contingency planning elements.

4.3. References

4.4. Attachments